REMARKS

This amendment is responsive to the Office Action mailed May 22, 2006. Reconsideration is requested in view of the amendments and remarks herein.

Claims 1-43 are pending.

Claims 1-43 stand rejected.

Claims 9, 10, 31 and 32 are cancelled.

Claims 44-46 are herein added.

Claims 1, 20, 24 and 40-43 are independent.

Claims 1, 11, 20, 24 and 40-43 are herein amended.

Formalities:

The drawings have been objected to because of inconsistencies with reference numerals. Applicant thanks the Examiner for his observations, and the specification has been amended accordingly to correct inconsistencies with reference numerals. Claim 20 has been amended as per the Examiner's suggestion to clarify the role of the security policy.

Rejection under 35 U.S.C. § 101:

The Office Action Rejects claim 42 because of non-statutory subject matter. Claim 42 has been herein amended to recite a "computer readable medium operable to store computer program logic embodied in computer program code encoded thereon for security enforcement for a persistent data repository." The claimed configuration is now clearly within statutory computer program subject matter to produce a tangible result. It is therefore respectfully requested that the rejection under 35 U.S.C. § 101 be withdrawn.

Rejection under 35 U.S.C. § 102 Based on Cook, U.S. Patent No. 6,820,082:

The Office Action rejects independent claims 1, 24 and 41-43 based on Cook et al. 6,820,082. Cook, however, is inapplicable to the method of claim 1 because Cook '082 does not show, teach, or disclose intercepting in a nonintrusive manner as claimed in Claim 1.

In the invention defined by the present claims, security is provided without disrupting the data flow or database communication. At a conceptual level, therefore, the claimed configuration is directed to a method that does not require being a party to the connection; the method "sniffs" and modifies the packets (requests and responses) rather than terminating the connection. The Cook approach talks about a proxy method, in which such operation is performed by operations on only the request and/or response, and not the data repository (i.e. database) itself. The disclosed configuration merely monitors and reports, and optionally either limits the query or the response, but in neither takes invasive measures that disrupt the connection or detectably modify the packet.

The Cook '082 system operates as an intermediary that intercepts all communications and directly affects the data whereas, in contrast, the configuration of Claim 1 is not a party to the communication in any way and merely inspects the incoming request in a non-intrusive manner to apply the rules to inspect and optionally, either allow the communication through or not. Therefore, the configuration of Claim 1 does not perform an action with respect to the data stored – rather, it merely perform a nonintrusive action on the connection and the request – distinct from manipulations and operations of the data in the database occurring from the application code in the server. The claimed mechanism is never a party to the database connection pair and is therefore non-intrusive to the database connection.

Accordingly, Claim 1 has been herein amended with the subject matter of claims 10 and 11 to clarify the nonintrusive and nondestructive nature of intervention. Amended Claim 1 now recites "interrogating and modifying the packets in a nondestructive manner with respect to the layered protocols," to further clarify and distinguish claim 1.

Further, claims 9 and 32, disclosing a configuration employing a proxy, have been herein cancelled, to further clarify and distinguish Applicant's claimed invention.

Claim 43 has been herein added, incorporating the subject matter of claims 1, 8, 15, 17 and 18, to further clarify the non-intrusive operation in a separate network device distinct from the application code of the scrutinized system, to further clarify and distinguish the configuration of claim 1.

Rejection under 35 U.S.C. § 103(a) Based on Cook, U.S. Patent No. 6,820,082 in view of Bechtolsheim, U.S. Patent No. 7,043,541:

The Office Action further rejects claims 10 and 11 under 35 U.S.C. § 103(a) based on Bechtolsheim, U.S. Patent No. 7,043,541. Bechtolsheim '541, however, is inapplicable to the configuration of claim 10 because Bechtolsheim destructively modifies the packet, by inserting a header in place of a preamble within the packet (Col. 2, lines 53-55). Thus, the Bechtolsheim method supercedes the original packet preamble with a standard preamble at a destination egress node, thus obliterating the contents of the former original packet preamble.

Further, even if one were to augment Cook '082 with the packet modification of Bechtolsheim, the result would not yield the claimed configuration because the Bechtolsheim approach supercedes the preamble and therefore is neither nonintrusive nor undetectable. In other words, Bechtolsheim modifies the packet header whereas claimed configurations may only modify the packet body but leave the packet header as is.

In further detail, Bechtolsheim discloses replacing a preamble with a modified header to provide support for network management (col. 3, lines 40-46). Bechtolsheim '541 therefore shows replacing control information with different control information so as to substantively change the packet for different action by the recipient. In contrast, the claimed packet modification is to complement or compensate for restrictions such that the resulting packet appears UNCHANGED to the recipient. Claim 46 has been herein added to recite "nondestructively modifying a payload of the packet, and leaving control information in the packet undisturbed," to further clarify the notion that the present invention does not modify control information.

Therefore, the claimed padding is to ensure similar treatment by the recipient as the unpadded packet would have received, to avoid detection or perception of the any detection or limiting performed. The Bechtolsheim padding, in contrast, enables a CDL header to replace the Ethernet preamble specifically to effect different treatment of packets between edge boundaries of a network, as discussed at col. 8, lines 15-55. Accordingly, Claim 1 has been amended with the subject matter of Claim 10, to recite that the modification to the packets is performed in a nondestructive manner, to further clarify the present configuration. Further, claim 45 has been herein added, depending from claim 1, reciting that "padding the packet further comprises nondestructively modifying the packet such that the packet appears undisturbed to the receiver," to further clarify and distinguish the present invention.

With respect to Claim 24, rejected on similar grounds as claim 1, Cook teaches an integrated system having a GUI specifically designed to receive a query operable for scrutiny, and appends SQL text to modify the query according to the rules, as disclosed at col. 5, lines 6-12. The Cook GUI, therefore, is customized to limit the received query to a limited scope for which the rule engine is adapted to scrutinize. In other words, the scrutiny or inspection of the Cook '082 system is limited to the fields provided by the integrated GUI.

In contrast, the claimed system is operable externally and independently from the scrutinized, or target system by undetectable intercepting network transmissions to the query engine, a process colloquially known as "sniffing the wire." The method of Claim 1 is not bound to a predetermined GUI for supplying anticipated files in an expected form, but is generally applicable to transactions generated by a user and directed to a database, as disclosed at page 3, lines 14-23, and further at page 16, line 20-page 17, line 12. Accordingly, it is submitted that Cook '082 does not show, teach, or disclose a limiter for limiting the data access transaction such that data indications (i.e. data references or items) are modified in a resulting data access transaction, as claimed in claim 24.

Further, Claim 24 has been amended with the subject matter of claim 31 to recite a "nonintrusive manner such that modifications performed on the data access transaction are undetectable to the user application and undetectable to the data repository," to further clarify and distinguish the arrangement of Claim 24. Cook '082 does not show, teach or disclose modifying the data access transaction as recited in claim 24. Rather, Cook modifies the actual data and data access operations in an active manner, rather than performing passive operations on the data access transaction. In Cook '082, the access manager 86 is integrated in the rule engine 78 between the user interface 76 and the database 74. Thus, the rule engine and corresponding rule application is an integral part of the user application and data repository. Accordingly, it is submitted that for these reasons and for the reasons cited above with respect to claim 1, the rule engine and corresponding rule application is not undetectable to the user application and data repository.

Rejection under 35 U.S.C. § 103(a) Based on Cook, U.S. Patent No. 6,820,082 in view of Slutz (U.S. Patent No. 6,581,052):

Claim 41 has been rejected under 35 U.S.C. § 102 based on Cook. Claim 41 has been herein amended with the subject matter of claim 13, to further clarify the present invention.

With respect to Claims 13 and 40, rejected under 35 U.S.C. § 103(a) based on Slutz (U.S. Patent No.6,581,052), Slutz is not applicable to the claimed configuration because Slutz '052 discloses test systems, not security implementations. Slutz discloses automated high-volume generation of SQL statements for test purposes (col. 4, line 66-Col. 5, line 2). Slutz is therefore nonanalogous art. The claimed invention receives and observes SQL statements; it does not generate them.

Further, the Slutz '052 system builds the structure of the parse tree first, then converts the parse tree to SQL statements (Col. 12, lines 39-48). In contrast, Claim 13 recites building the parse tree from the SQL statement. Thus, Slutz discloses the reverse operation from Claim 13. Therefore, one of skill in the art would not look to Slutz '052 to modify Cook '082, and further if one did combine the SQL generation of Slutz with Cook., the result would be inoperable because there would be no initial SQL statement for which to apply the Cook method. Claim 40 has been further amended to recite "modifying the packet content being delivered to the database consistent with the original data retrieval request," to clarify the nonintrusive nature of the modification, as discussed above. Independent Claim 20 has been likewise amended with the subject matter of claim 13, and is therefore submitted as allowable.

Claim 42 stands rejected for reasons similar to claim 1. Claim 42 has been amended with the subject matter of claims 17 and 18, to further distinguish claim 42 over Cook.

The Office Action further rejects Claims 17 and 18 under 35 U.S.C. § 102. Cook '082, however, discloses a rule engine integrated with the user interface and the data access manager on a common application server. The claimed security filter component is a separate network device that differs from the application server in Cook because the claimed configuration disposes the rule based processing entity (rule engine) before the GUI. In contrast, the Cook rule engine is disposed between the user interface and the database, thus the user interface is responsive to the rule engine for gathering appropriate fields and information (Col. 5, lines 42-61). The claimed component separate from the source and destination is independent of the data access transaction, and thus has no control to collect specific fields or otherwise direct the generation of the data access request.

Claim 43 has been rejected for reasons similar to Claim 1. Claim 43 has been amended with the subject matter of claims 5 and 6, to further clarify and distinguish the present invention.

However, the Office Action further rejects claims 5 and 6 under 35 U.S.C. § 103(a) based on Fisher (U.S. Patent No. 6,085,191). Fisher '191 discloses database views, which limit a particular user's access to objects, typically rows, defined by the views. As indicated above, the claimed system scrutinizes the transaction, to determine what the user may see (i.e. data level security), rather than an access control mechanism, which selectively enables code to distinguish which object the user may manipulate.

In Cook '082, the cited row limiting occurs by narrowing the selection of the query REQUEST to fetch fewer rows, not by eliminating already fetched rows in the query RESPONSE. Cook '082 narrows the SQL selection by appending additional selection qualifiers to the SQL statement to form a modified SQL Query (Col. 8, lines 40-53). In contrast, the claimed limiting occurs by filtering selected rows from the already fetched row set, after retrieval from the database query. Accordingly, Claim 43 has been herein amended with the subject matter of Claims 5 and 6 to recite that limiting of the data query response includes "selectively eliminating rows in the row set including the restricted data items, based on the comparing, to generate a modified query response including a filtered row set," as now recited in amended Claim 43. Claim 43 has been further amended with the subject matter of claims 8, 10, and 11, as discussed above, to further clarify the nonintrusive and nondestructive features of data access transaction scrutiny.

As the remaining claims all depend, either directly or indirectly from claims 1, 20, and 24, which by the foregoing are deemed allowable, it is respectfully submitted that all claims are now in condition for allowance.

Applicant(s) hereby petition(s) for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3735.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-9660, in Westborough, Massachusetts.

Respectfully submitted,

Christopher J. Lutz, Esq.
Attorney for Applicant(s)
Registration No.: 44,883
Chapin Intellectual Property Law, LLC
Westborough Office Park
1700 West Park Drive
Westborough, Massachusetts 01581
Telephone: (508) 616-9660
Facsimile: (508) 616-9661

Attorney Docket No.: GRD03-01

Dated: August 9, 2006